Roles and User Groups

This chapter provides information about roles and user groups in Cisco Unified Communications Manager Administration which uses roles and user groups to provide varying levels of privilege (access). This technique permits granting only the required privileges for a selected group of users and limits the configuration functions that users in a particular user group can perform.

Overview

Roles and user groups provide multiple levels of security to Cisco Unified Communications Manager Administration and to other applications. The system groups the resources that are available to Cisco Unified Communications Manager Administration and to other applications into roles. Each application comes with standard, predefined roles. Each application defines its own access privilege for Cisco Unified Communications Manager Administration.

Administrators can configure additional roles for an application. A role contains, for a particular application, the list of resources that an application comprises. For each resource that a role comprises, the administrator defines the access privilege. For the Cisco Unified Communications Manager Administration application, the access privileges include read and update. Other applications specify their own access privileges.

Because Cisco Unified Communications Manager allows administrators to manage user groups, roles, and resources, no guarantee exists that a particular user group or role goes unchanged or that administrators will use the predefined user groups or roles.

Roles

The system groups the resources that are available to Cisco Unified Communications Manager Administration and to other applications into roles. A role includes a collection of resources for an application, such as Cisco Unified Communications Manager Administration. The following types of roles exist:

- Custom roles-Administrator-defined roles that you configure in Cisco Unified Communications Manager Administration after a Cisco Unified Communications Manager installation; for example, a help desk role.

- Standard roles-Default roles that get created automatically with Cisco Unified Communications Manager installation; you cannot modify or delete standard roles, but you can copy them to create custom roles, which allows you to modify them for your preferences. (See the table below for the list of standard roles and the privileges/resources that the role provides.)

Each role contains a group of resources, with privileges assigned to each resource. For most applications with graphical user interfaces, such as Cisco Unified Communications Manager Administration, privileges allow you to perform tasks, such as viewing or updating data, in a specific window or a group of related windows, which are defined as resources in the Role Configuration window. For example, for the Standard CCM Feature Management role, you can view and configure message waiting in the Message Waiting Configuration window in Cisco Unified Communications Manager Administration. For each role that is associated with Cisco Unified Communications Manager Administration, the specified privilege allows a certain level of access to each of the resources (windows). For example, privileges specify the following access in Cisco Unified Communications Manager Administration:

- Read- Allows users in a user group to view data in specific windows (defined as resources), but the user(s) cannot modify data in the window. Buttons such as Insert, Delete, Update, and Reset do not display.

- Update-Allows users in a user group to view and modify data in certain windows (defined as resources for the role). Users with the update privilege can perform operations such as Insert, Delete, Update, and Reset.

Other applications, such as CTI applications, specify their own access privileges and do not use the read and update privileges or a common list of resources (which are configuration windows in most cases); for example, the Standard CTI Allow Call Recording role allows CTI devices/CTI applications to record calls, and the Standard EM Authentication Proxy Rights manages Cisco Extension Mobility authentication rights for application users that interact with Cisco Extension Mobility.

Note The Standard CCM Admin Users role gives the user access to the Cisco Unified Communications Manager Administration user interface. This role, the base role for all administration tasks, serves as the authentication role. Cisco Unified Communications Manager Administration defines this role as the role that is necessary to log in to Cisco Unified Communications Manager Administration.

The Standard CCM Admin Users role includes no permissions beyond logging into Cisco Unified Communications Manager Administration. The administrator must add another authorization role to define the parts of the Cisco Unified Communications Manager Administration that the user can administer. The Standard CCMADMIN Administration role allows a user to access and make changes in all of Cisco Unified Communications Manager Administration.

✎

Note   A user with only the Standard CCM Admin Users role can access Cisco Unified Communications Manager Administration but cannot make any changes. A user with only the Standard CCMADMIN Administration role can make changes, but cannot authenticate entry to Cisco Unified Communications Manager Administration.

A user, therefore, must have the Standard CCM Admin Users role to access Cisco Unified Communications Manager Administration and must have at least one other role to administer the system.

The following table lists the standard roles, the application(s) that the roles support, the privileges (resources) for the roles, and the standard user groups that are automatically associated with the standard roles.

⚠

Caution   For a role, supported privileges are checked in the Role Configuration window. For standard roles, you cannot change the configuration, but if you want to do so, you can copy a standard role to configure a custom role, which you can modify to your preferences.

Table 1: Standard Roles and Privileges

Standard Role	Supported Application(s)	Privileges/Resources for the Role	Associated Standard User Group(s)
Standard AXL API Access	AXL database API	Allows access to the AXL database API	Standard CCM Super Users
Standard Admin Rep Tool Admin	Cisco Unified Communications Manager CDR Analysis and Reporting (CAR)	Allows an administrator to view and configure Cisco Unified Communications Manager CDR Analysis and Reporting (CAR).	Standard CAR Admin Users, Standard CCM Super Users
Standard Audit Log Administration	Cisco Unified Serviceability	Allows an administrator to perform the following tasks for the audit logging feature: • View and configure audit logging in the Audit Log Configuration window in Cisco Unified Serviceability • View and configure trace in Cisco Unified Serviceability and collect traces for the audit log feature in Real-Time Monitoring Tool • View and start/stop the Cisco Audit Event service in Cisco Unified Serviceability • View and update the associated alert in RTMT	Standard Audit Users

Standard Role	Supported Application(s)	Privileges/Resources for the Role	Associated Standard User Group(s)
Standard CCM Admin Users	Cisco Unified Communications Manager Administration	Grants log-in rights to Cisco Unified Communications Manager Administration.	Standard CCM Admin Users, Standard CCM Gateway Administration, Standard CCM Phone Administration, Standard CCM Read Only, Standard CCM Server Monitoring, Standard CCM Super Users, Standard CCM Server Maintenance, Standard Packet Sniffer Users
Standard CCM End Users	Cisco Unified Communications Self Care Portal	Grant an end user log-in rights to the Cisco Unified Communications Self Care Portal **Tip** After you configure the user, make sure that you add the user to the Standard CCM End Users user group (**User Management** > **User Group**). If you do not add the user to this group, the user cannot view and update the Cisco Unified Communications Self Care Portal.	Standard CCM End Users

Standard Role	Supported Application(s)	Privileges/Resources for the Role	Associated Standard User Group(s)
Standard CCM Feature Management	Cisco Unified Communications Manager Administration	Allows an administrator to perform the following tasks: • View, delete, and insert the following items by using the Bulk Administration Tool: 　◦ Client matter codes and forced authorization codes 　◦ Call pickup groups • View and configure the following items in Cisco Unified Communications Manager Administration: 　◦ Client matter codes and forced authorization codes 　◦ Call park 　◦ Call pickup 　◦ Meet-Me numbers/patterns 　◦ Message Waiting 　◦ Cisco Unified IP Phone Services 　◦ Voice mail pilots, voice mail port wizard, voice mail ports, and voice mail profiles	Standard CCM Server Maintenance
Standard CCM Gateway Management	Cisco Unified Communications Manager Administration	Allows an administrator to perform the following tasks: • View and configure gateway templates in the Bulk Administration Tool • View and configure gatekeepers, gateways, and trunks in Cisco Unified Communications Manager Administration	Standard CCM Gateway Administration

Standard Role	Supported Application(s)	Privileges/Resources for the Role	Associated Standard User Group(s)

Standard CCM Phone Management	Cisco Unified Communications Manager Administration	Allows an administrator to perform the following tasks:
		
		• View and export phones in the Bulk Administration Tool
		
		• View and insert user device profiles in the Bulk Administration Tool
		
		• View and configure the following items in Cisco Unified Communications Manager Administration:
		
		  ◦ BLF speed dials
		
		  ◦ CTI route points
		
		  ◦ Default device profiles or default profiles
		
		  ◦ Directory numbers and line appearances
		
		  ◦ Firmware load information
		
		  ◦ Phone button templates or softkey templates
		
		  ◦ Phones
		
		  ◦ Reorder phone button information for a particular phone by clicking the Modify Button Items button in the Phone Configuration window
			Standard CCM Phone Administration

Standard Role	Supported Application(s)	Privileges/Resources for the Role	Associated Standard User Group(s)
Standard CCM Route Plan Management	Cisco Unified Communications Manager Administration	Allows an administrator to perform the following tasks in Cisco Unified Communications Manager Administration: • View and configure application dial rules • View and configure calling search spaces and partitions • View and configure dial rules, including dial rule patterns • View and configure hunt lists, hunt pilots, and line groups • View and configure route filters, route groups, route hunt list, route lists, route patterns, and route plan report • View and configure time period and time schedule • View and configure translation patterns	

Standard CCM Service Management	Cisco Unified Communications Manager Administration	Allows an administrator to perform the following tasks:
		
		• View and configure the following items in Cisco Unified Communications Manager Administration:
		
		  ◦ Annunciators, conference bridges, and transcoders
		
		  ◦ MOH audio sources and MOH servers
		
		  ◦ Media resource groups and media resource group lists
		
		  ◦ Media termination point
		
		  ◦ Cisco Unified Communications Manager Assistant wizard
		
		• View and configure the Delete Managers, Delete Managers/Assistants, and Insert Managers/Assistants windows in the Bulk Administration Tool
			Standard CCM Server Maintenance

Standard Role	Supported Application(s)	Privileges/Resources for the Role	Associated Standard User Group(s)

Standard CCM System Management	Cisco Unified Communications Manager Administration	Allows an administrator to perform the following tasks:
		• View and configure the following items in Cisco Unified Communications Manager Administration:
		  ◦ AAR groups
		  ◦ Cisco Unified Communications Managers (Cisco Unified CMs) and Cisco Unified Communications Manager groups
		  ◦ Date and time groups
		  ◦ Device defaults
		  ◦ Device pools
		  ◦ Enterprise parameters
		  ◦ Enterprise phone configuration
		  ◦ Locations
		  ◦ NTP servers
		  ◦ Plug-ins
		  ◦ Security profiles for phones that run SCCP or SIP; security profiles for SIP trunks
		  ◦ SRST references
		  ◦ Servers
		• View and configure the Job Scheduler windows in the Bulk Administration Tool
			Standard CCM Server Maintenance

Standard CCM User Privilege Management	Cisco Unified Communications Manager Administration	Allows an administrator to view and configure application users in Cisco Unified Communications Manager Administration.	
Standard CCMADMIN Administration	Cisco Call Manager IM and Presence Administration	Allows an administrator access to all aspects of the CCMAdmin system	
Standard CCMADMIN Administration	Cisco Unified Communications Manager Administration	Allows an administrator to view and configure all items in Cisco Unified Communications Manager Administration and the Bulk Administration Tool.	Standard CCM Super Users

Standard Role	Supported Application(s)	Privileges/Resources for the Role	Associated Standard User Group(s)
Standard CCMADMIN Administration	Dialed Number Analyzer	Allows an administrator to view and configure information in Dialed Number Analyzer.	
Standard CCMADMIN Read Only	Cisco Call Manager IM and Presence Administration	Allows read access to all CCMAdmin resources	
Standard CCMADMIN Read Only	Cisco Unified Communications Manager Administration	Allows an administrator to view configuration in Cisco Unified Communications Manager Administration and the Bulk Administration Tool.	Standard CCM Gateway Administration, Standard CCM Phone Administration, Standard CCM Read Only, Standard CCM Server Maintenance, Standard CCM Server Monitoring
Standard CCMADMIN Read Only	Dialed Number Analyzer	Allows an administrator to analyze routing configurations in Dialed Number Analyzer.	
Standard CCMUSER Administration	Cisco Unified Communications Self Care Portal	Allows access to the Cisco Unified Communications Self Care Portal.	Standard CCM End Users
Standard CTI Allow Call Monitoring	Cisco Computer Telephone Interface (CTI)	Allows CTI applications/devices to monitor calls	Standard CTI Allow Call Monitoring
Standard CTI Allow Call Park Monitoring	Cisco Computer Telephone Interface (CTI)	Allows CTI applications/devices to use call park	Standard CTI Allow Call Park Monitoring
Standard CTI Allow Call Recording	Cisco Computer Telephone Interface (CTI)	Allows CTI applications/devices to record calls	Standard CTI Allow Call Recording
Standard CTI Allow Calling Number Modification	Cisco Computer Telephone Interface (CTI)	Allows CTI applications to transform calling party numbers during a call	Standard CTI Allow Calling Number Modification
Standard CTI Allow Control of All Devices	Cisco Computer Telephone Interface (CTI)	Allows control of all CTI-controllable devices	Standard CTI Allow Control of All Devices
Standard CTI Allow Control of Phones Supporting Connected Xfer and conf	Cisco Computer Telephone Interface (CTI)	Allows control of all CTI devices that supported connected transfer and conferencing	Standard CTI Allow Control of Phones supporting Connected Xfer and conf

Standard Role	Supported Application(s)	Privileges/Resources for the Role	Associated Standard User Group(s)
Standard CTI Allow Control of Phones Supporting Rollover Mode	Cisco Computer Telephone Interface (CTI)	Allows control of all CTI devices that supported Rollover mode	Standard CTI Allow Control of Phones supporting Rollover Mode
Standard CTI Allow Reception of SRTP Key Material	Cisco Computer Telephone Interface (CTI)	Allows CTI applications to access and distribute SRTP key material	Standard CTI Allow Reception of SRTP Key Material
Standard CTI Enabled	Cisco Computer Telephone Interface (CTI)	Enables CTI application control	Standard CTI Enabled
Standard CTI Secure Connection	Cisco Computer Telephone Interface (CTI)	Enables a secure CTI connection to Cisco Unified Communications Manager	Standard CTI Secure Connection
Standard CUReporting	Cisco Call Manager IM and Presence Reporting	Allows application users to generate reports from various sources	
Standard CUReporting	Cisco Unified Reporting	Allows an administrator to view, download, generate, and upload reports in Cisco Unified Reporting	Standard CCM Administration Users, Standard CCM Super Users
Standard EM Authentication Proxy Rights	Cisco Extension Mobility	Manages application Cisco Extension Mobility authentication rights; required for all application users that interact with Cisco Extension Mobility (for example, Cisco Unified Communications Manager Assistant and Cisco Web Dialer)	Standard CCM Super Users, Standard EM Authentication Proxy Rights
Standard Packet Sniffing	Cisco Unified Communications Manager Administration	Allows an administrator to access Cisco Unified Communications Manager Administration to enable packet sniffing (capturing)	Standard Packet Sniffer Users
Standard RealtimeAndTraceCollection	Cisco Unified Serviceability and Real-Time Monitoring Tool	Allows an administrator to view and use the SOAP Serviceability AXL APIs, the SOAP Call Record APIs, the SOAP Diagnostic Portal (Analysis Manager) Database Service; view and configure trace for the audit log feature, and view and configure the Real-Time Monitoring Tool, including collecting traces in RTMT.	Standard RealtimeAndTraceCollection

Standard Role	Supported Application(s)	Privileges/Resources for the Role	Associated Standard User Group(s)
Standard SERVICEABILITY	Cisco Unified Serviceability and Real-Time Monitoring Tool	Allows an administrator to view and configure the following windows in Cisco Unified Serviceability or the Real-Time Monitoring Tool: • Alarm Configuration and Alarm Definitions (Cisco Unified Serviceability) • Audit Trace (marked as read/view only) • SNMP-related windows (Cisco Unified Serviceability) • Trace Configuration and Troubleshooting Trace Configuration (Cisco Unified Serviceability) • Log Partition Monitoring • Alert Configuration (RTMT), Profile Configuration (RTMT), Trace Collection (RTMT) Allows an administrator to view and use the SOAP Serviceability AXL APIs, the SOAP Call Record APIs, and the SOAP Diagnostic Portal (Analysis Manager) Database Service. **Tip** For the SOAP Call Record API, the RTMT Analysis Manager Call Record permission is controlled through this resource. **Tip** For the SOAP Diagnostic Portal Database Service, the RTMT Analysis Manager Hosting Database access controlled thorough this resource.	Standard CCM Server Monitoring, Standard CCM Super Users
Standard SERVICEABILITY Administration	Cisco Unified Communications Manager Administration	A serviceability administrator can access the Plugin window in Cisco Unified Communications Manager Administration and download plugins from this window.	
Standard SERVICEABILITY Administration	Dialed Number Analyzer	Allows an administrator to administer all aspects of serviceability for Dialed Number Analyzer.	
Standard SERVICEABILITY Administration	Cisco Unified Serviceability and Real-Time Monitoring Tool	Allows an administrator to view and configure all windows in Cisco Unified Serviceability and RTMT. (Audit Trace supports viewing only.) Allows an administrator to view and use all SOAP Serviceability AXL APIs.	

Standard Role	Supported Application(s)	Privileges/Resources for the Role	Associated Standard User Group(s)
Standard SERVICEABILITY Read Only	Dialed Number Analyzer	Allows an administrator to view all serviceability-related data for components in Dialed Number Analyzer.	Standard CCM Read Only
Standard SERVICEABILITY Read Only	Cisco Unified Serviceability and Real-Time Monitoring Tool	Allows an administrator to view configuration in Cisco Unified Serviceability and RTMT. (excluding audit configuration window, which is represented by the Standard Audit Log Administration role) Allows an administrator to view all SOAP Serviceability AXL APIs, the SOAP Call Record APIs, and the SOAP Diagnostic Portal (Analysis Manager) Database Service.	
Standard System Service Management	Cisco Unified Serviceability	Allows an administrator to view, activate, start, and stop services in Cisco Unified Serviceability.	

User Groups

After configuration of custom roles, you can configure user groups, which are a collection of Cisco Unified Communications Manager application users and end users that get grouped together for the purpose of assigning a common list of roles to the members in the user group. Like standard roles, standard user groups get created at installation, and you cannot delete these user groups; you can only add or delete application or end users from standard user groups.

Standard user groups in Cisco Unified Communications Manager Administration provide a predefined set of roles and permissions for various functions. Administrators can manage user groups, roles, and permissions to control the level of access (and, therefore, the level of security) for system users.

Various named user groups that are predefined have no members that are assigned to them at install time. The Cisco Unified Communications Manager super user or a user with access to user group configuration should add users to these groups. The super user or a user with access to user group configuration can configure additional named user groups as needed.

Note The Standard CCM Super Users user group represents a named user group that always has full access permission to all named roles. You cannot delete this user group. You can only make additions and deletions of users to this group.

Note CCMAdministrator always represents a super user.

Certain user groups and roles exhibit limitations that administrators need to recognize. For example, you can modify the Standard EM Authentication Proxy Rights user group by adding both application users and end

users. Because authentication by proxy is intended for use by applications, end users that get added to this user group cannot authenticate by proxy.

Access Log

The log contains a file report of access/change attempts. That is, Cisco Unified Communications Manager Administration generates a record of attempts to access or modify any directory or database component through Cisco Unified Communications Manager Administration. The change record includes the user name, date, time, window from which the change was made, and the success or failure status of the update.

Enterprise Parameters

Roles and user groups use the Effective Access Privileges For Overlapping User Groups and Roles enterprise parameter.

Effective Access Privileges for Overlapping User Groups and Roles

The Effective Access Privileges For Overlapping User Groups and Roles enterprise parameter determines the level of user access for users that belong to multiple user groups and have conflicting privileges.

You can set this enterprise parameter to the following values:

- Maximum-The effective privilege represents the maximum of the privileges of all the overlapping user groups.
- Minimum-The effective privilege represents the minimum of the privileges of all the overlapping user groups.

The Effective Access Privileges For Overlapping User Groups and Roles enterprise parameter specifies the maximum default value.

> **Note** This enterprise parameter does not affect the privileges for the members of the Standard CCM Super Users user group.

Create a Custom Help Desk Role and User Group

Some companies want their help desk personnel to have privileges to be able to perform certain tasks, such as adding a phone, adding an end user, or adding an end user to a user group in Cisco Unified Communications Manager Administration.

Performing the steps in the following example allows help desk personnel to add a phone, add an end user, and add the end user to the Standard CCM End Users user group, which allows an end user to access and update the Cisco Unified Communications Self Care Portal.

Example-Allows Help Desk Personnel to Add Phone, Add End User, and Add End User to User Group

Procedure

Step 1 In Cisco Unified Communications Manager Administration, choose **User Management** > **Role**.

Step 2 Click **Add New**.

Step 3 From the Application drop-down list box, choose **Cisco Call Manager Administration**; then, click **Next**.

Step 4 In the Name field, enter the name of the role; for example, Help Desk.

Step 5 In the Description field, enter a short description; for example, for adding phones and users.

Step 6 Choose one of the following options, which depends on where you want the help desk personnel to perform the task:

a) If you want the help desk personnel to add a phone in the Phone Configuration window and then add an end user in the End User Configuration window. check the read and update privileges check boxes for the User web page resource and the Phone web pages resource; then, click **Save**.

b) If you want the help desk personnel to add both a phone and user at the same time in the User and Phone Add window, check the read and update privileges check boxes for the User and Phone add resource and the User web page resource; then click **Save**.

Step 7 By performing the following tasks, create a custom user group for the help desk:

a) In Cisco Unified Communications Manager Administration, choose **User Management** > **User Group**; then, click **Add New**.

b) Enter the name of the custom user group; for example, Help Desk.

c) From the Related Links drop-down list box, choose **Assign Roles to User Group**; then, click **Go**.

d) Click the **Assign Role to Group** button.

e) Check the check box for the custom role that you created in Step 6; in this example, Help Desk. In addition, check the check box for the Standard CCM Admin Users role. Then, click **Add Selected**.

f) In the User Group Configuration window, verify that the roles display in the Role Assignment pane; then, click **Save**.

What to Do Next

In Cisco Unified Communications Manager Administration, the help desk personnel can add the phone, add the user, and add the end user to the user group.

- To add a phone in the Phone Configuration window, choose **Device** > **Phone**; then, to add an end user in the End User Configuration window, choose **User Management** > **End User**.

- To add both a phone and user at the same time in the User and Phone Add window, choose **User Management** > **User and Phone Add**.

- To associate the end user with the Standard CCM End Users user group, choose **User Management** > **User Group**.